orange™ Business Services

Baromètre cybersécurité 2017
Où en est l'industrie française ?

« La transformation numérique des entreprises est devenue une condition majeure de leur croissance. En investissant dans les technologies de l'information, elles doivent cependant veiller à se protéger face à des cybermenaces en constante évolution. Pour les accompagner dans cette démarche, Orange Business Services a fait le choix de devenir un acteur européen de référence en réunissant son expertise en matière de sécurité numérique au sein d'une seule entité, Orange Cyberdefense. »

Michel Van Den Berghe
Président d'Orange Cyberdefense

Dans cette enquête réalisée par l'Usine Nouvelle pour Orange Business Services, les entreprises industrielles françaises dévoilent leurs risques numériques :

- Ont-elles subi des attaques durant l'année qui vient de s'écouler et quels en sont les impacts ?
- Se sentent-elles bien préparées ?
- Quelles sont les menaces qu'elles redoutent le plus ?
- Quelles solutions sont mises en place pour mieux se protéger ?

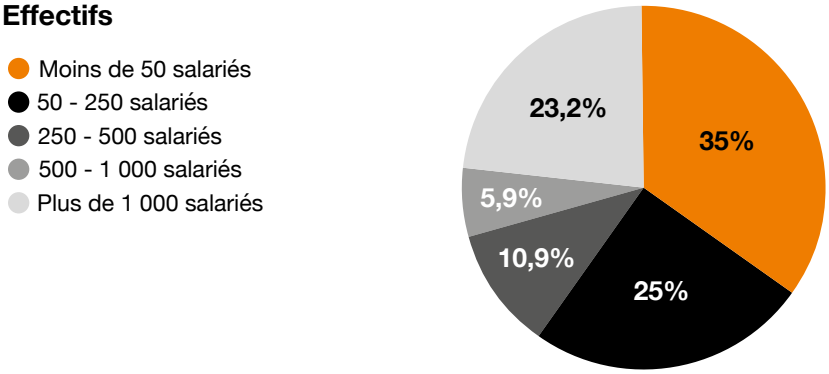
Découvrez ici l'ensemble des résultats du baromètre 2017 et les principaux changements par rapport à 2015, détaillés selon la taille des entreprises : plus de 1 000 salariés, de 250 à 1 000 salariés et moins de 250 salariés.

Enquête réalisée, du 8 au 24 novembre 2016, auprès de 347 dirigeants d'entreprises françaises du secteur de l'industrie.

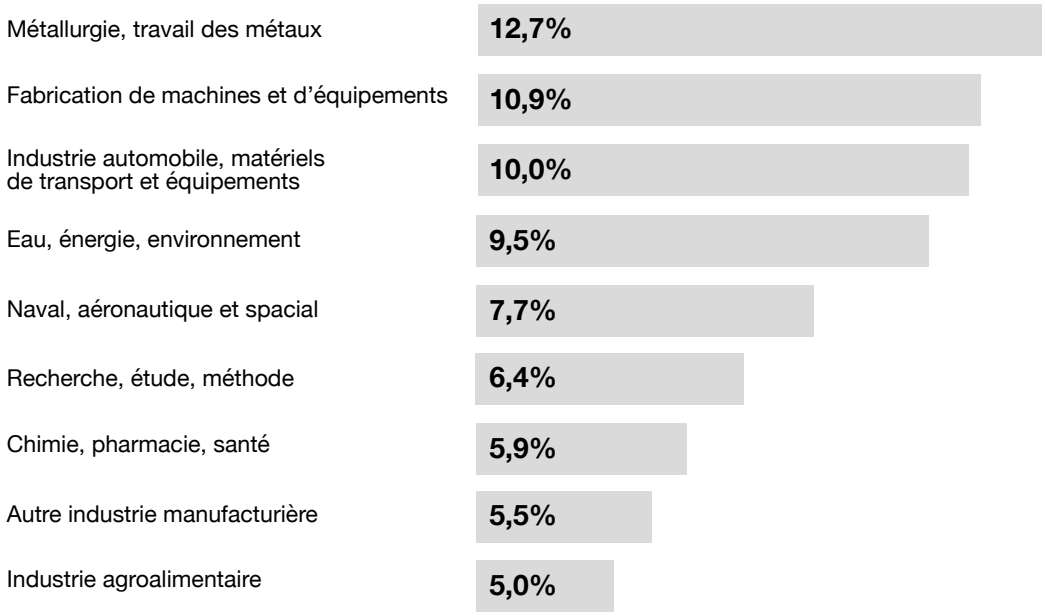
Sommaire

Le profil des répondants

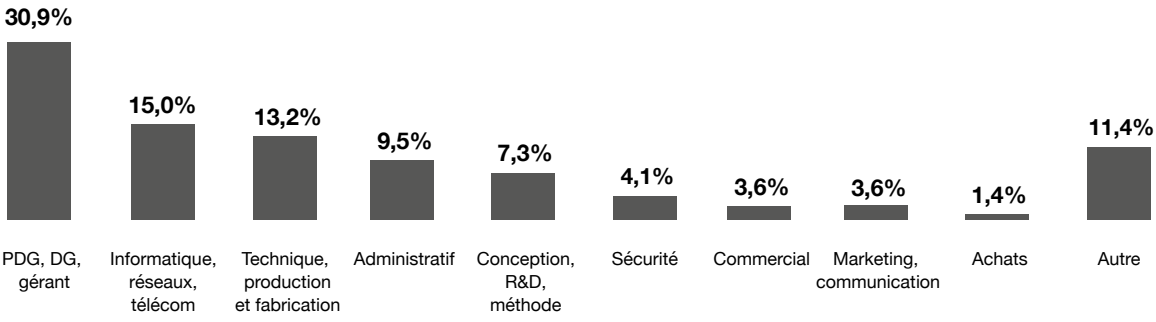
Effectifs



Secteurs

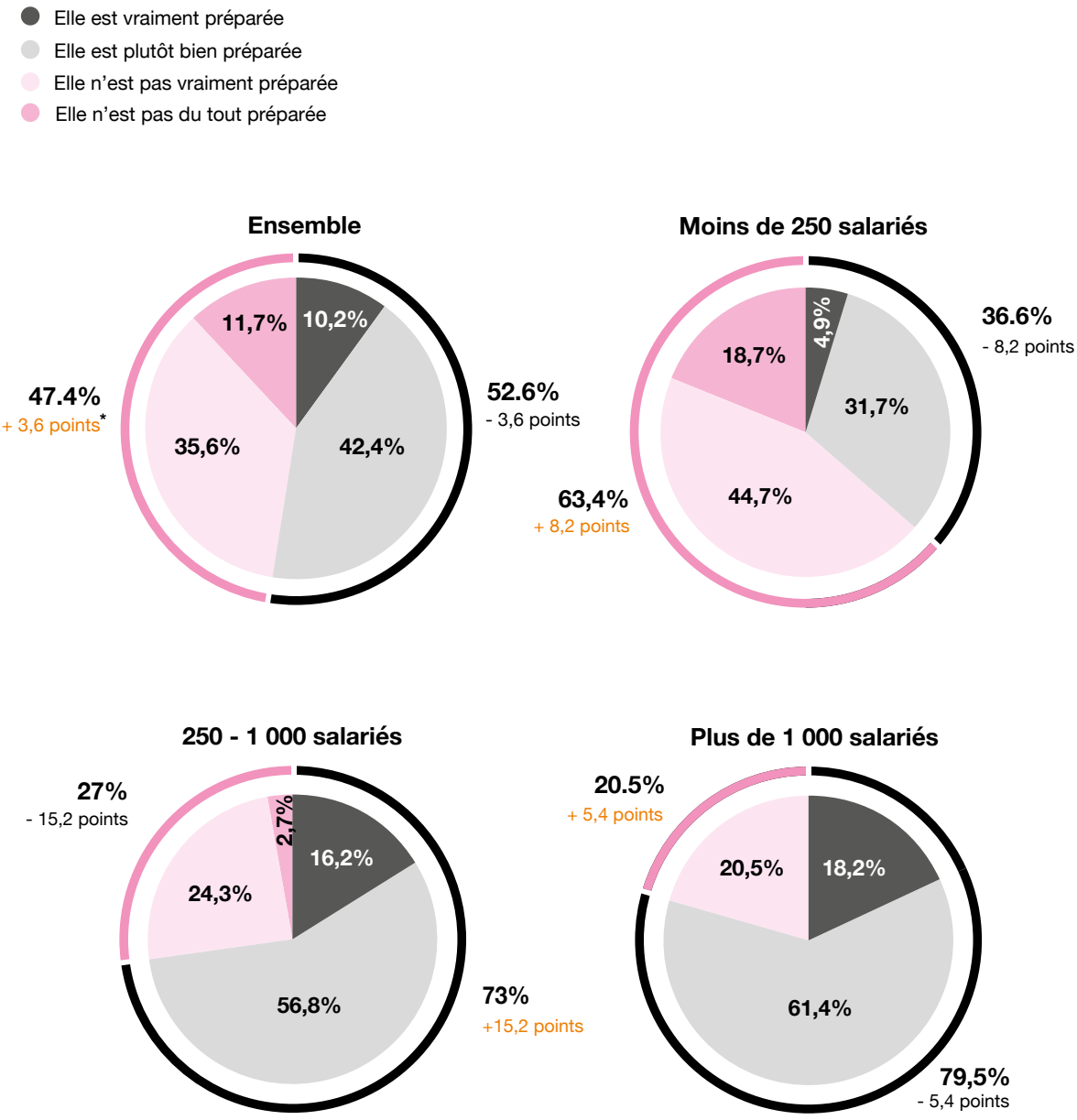


Fonctions



Les entreprises se sentent-elles préparées ?

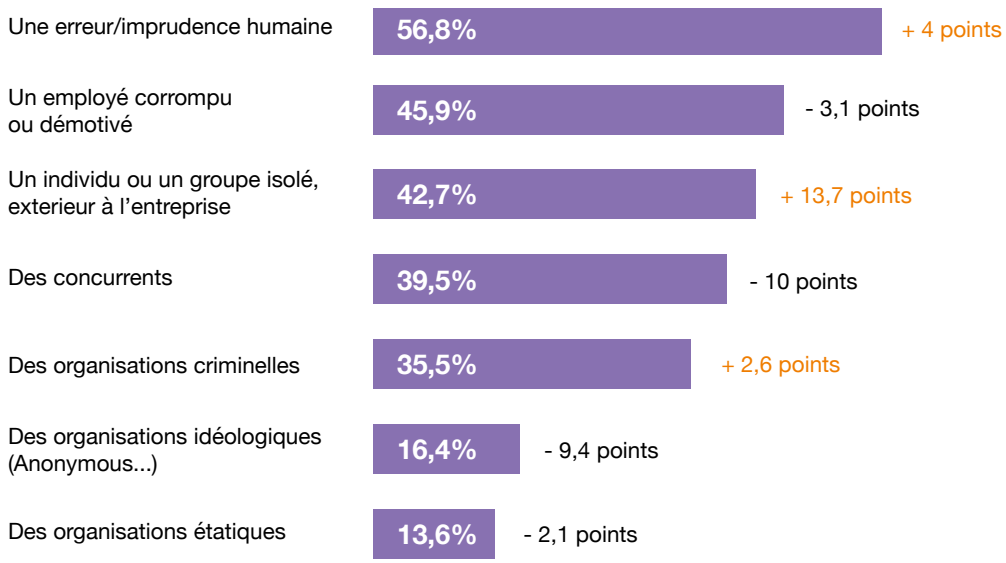
Votre entreprise est-elle bien préparée sur les questions de cybersécurité ?

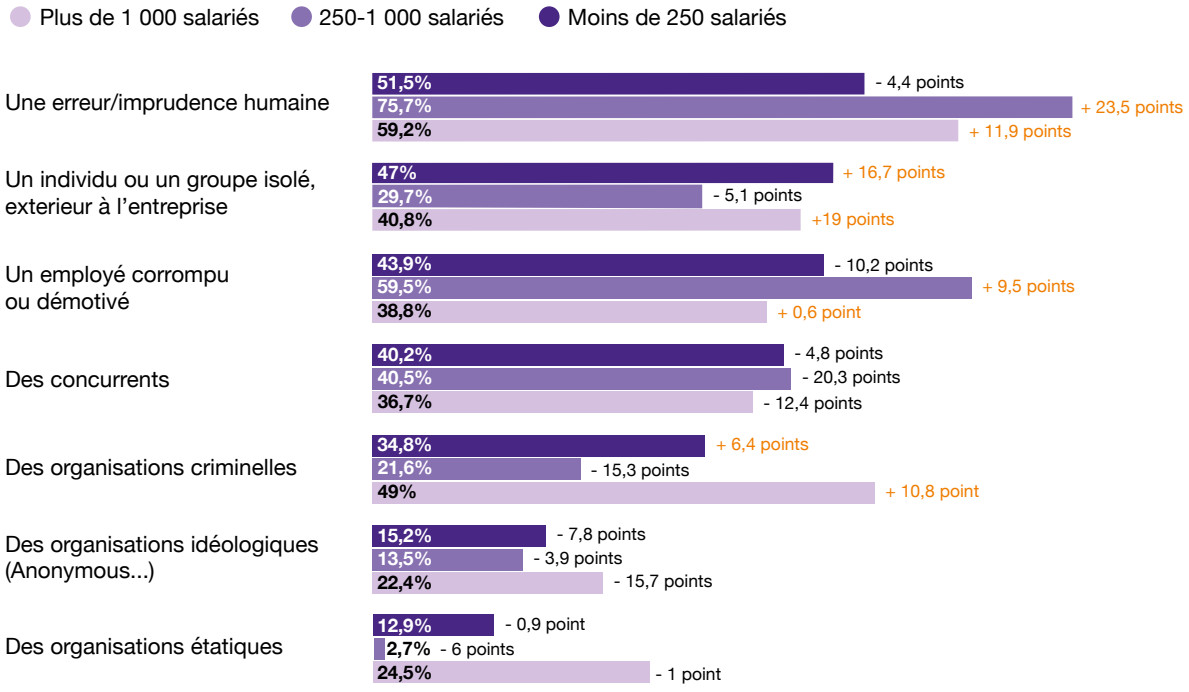


* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Les principales craintes

Parmi les menaces potentielles suivantes, lesquelles craignez-vous le plus ?

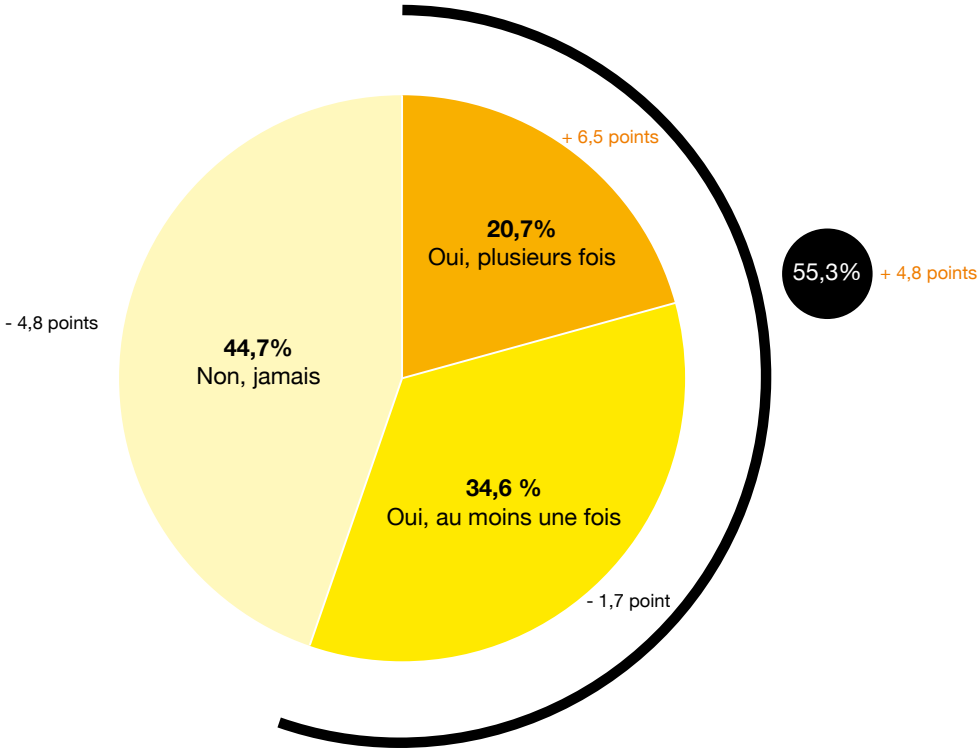


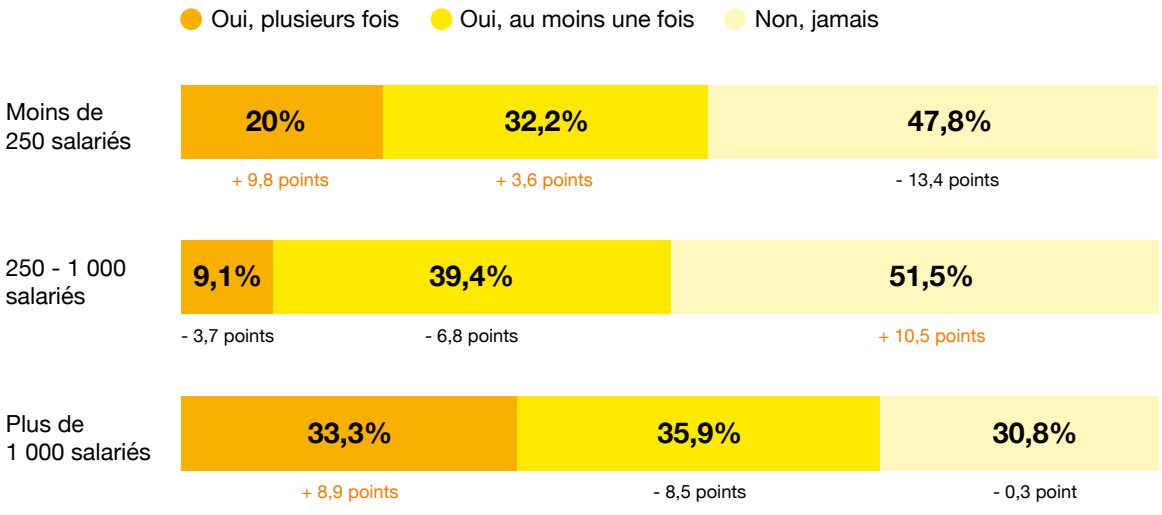


* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Les incidents rencontrés

Avez-vous été confronté à un/des incident(s) de cybersécurité au cours des 12 derniers mois dans votre entreprise ?

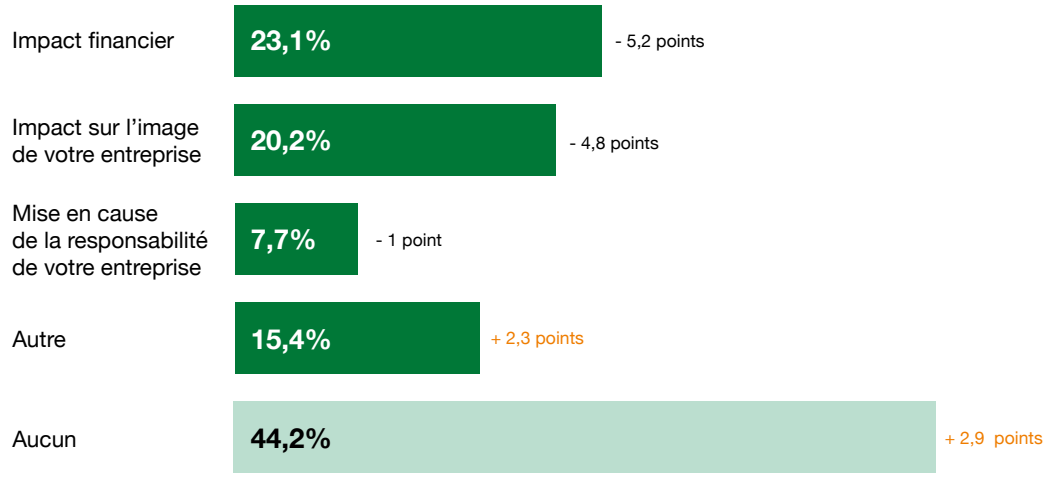


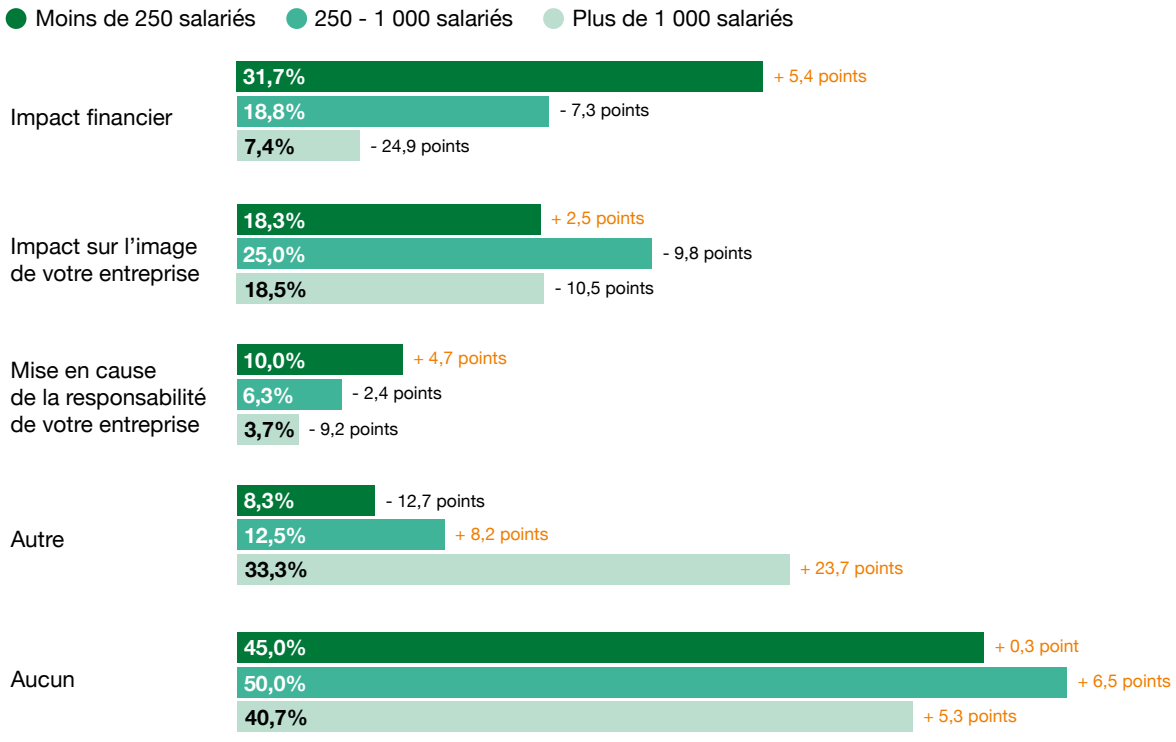


* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Les impacts subis par les entreprises

Concernant les cyberattaques que vous avez pu subir, pouvez-vous nous indiquer quel en a été l'impact ?

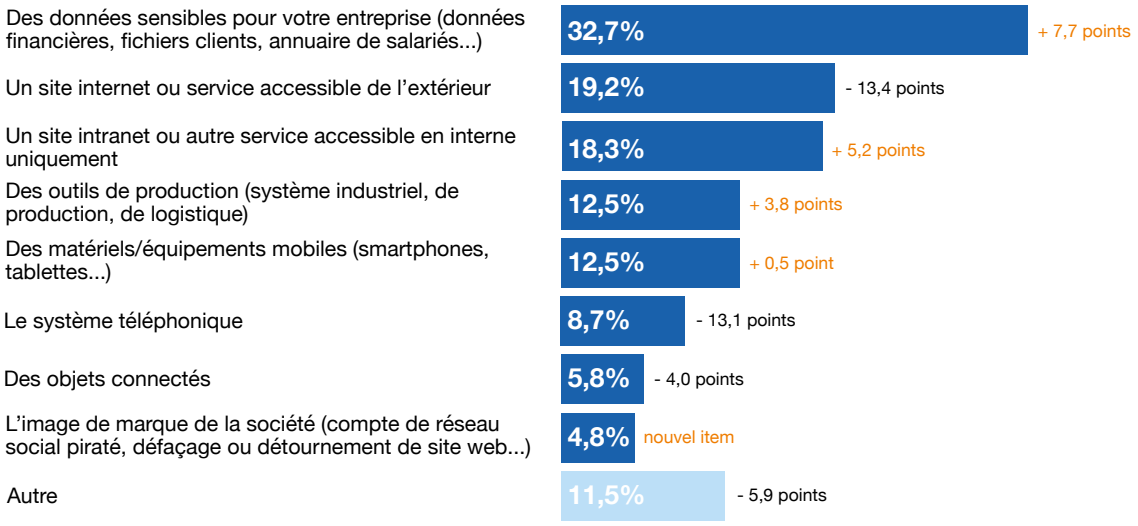


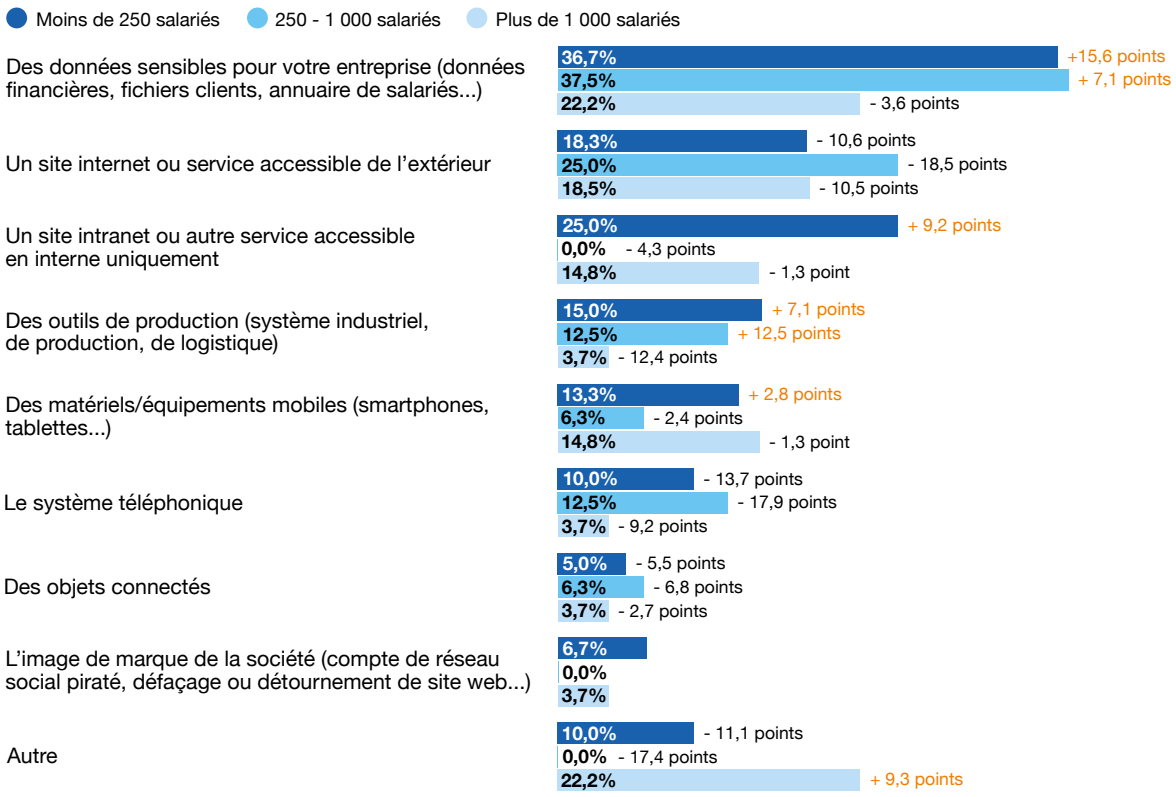


* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Les cibles des cyberattaques

Pouvez-vous nous indiquer ce qui a été ciblé ?

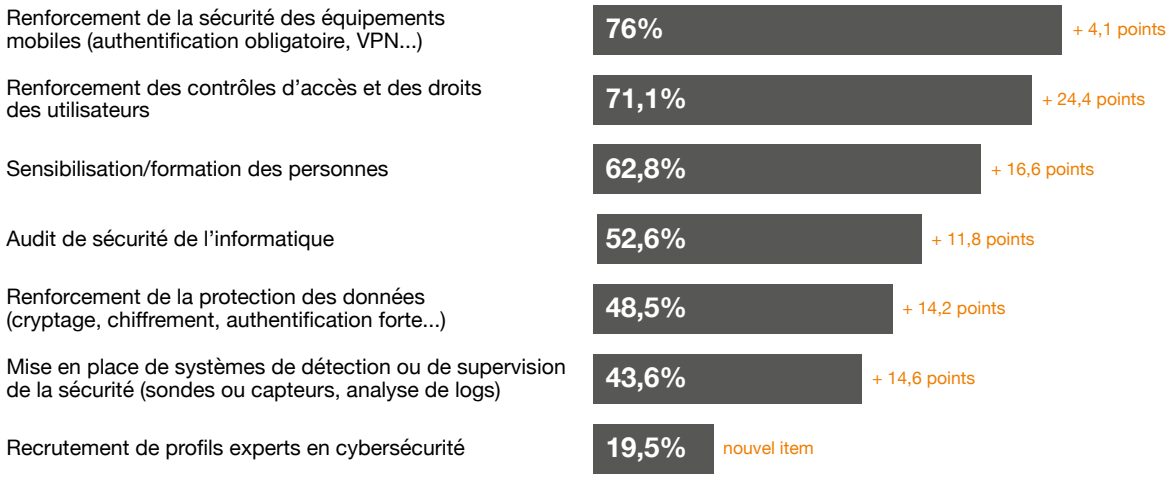


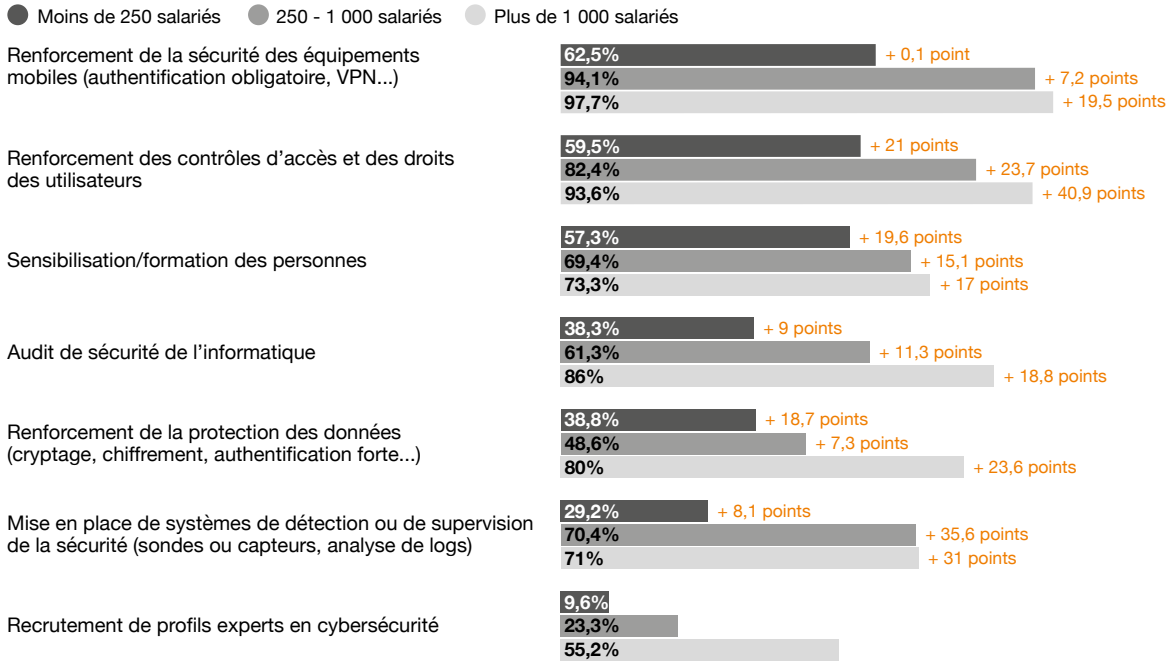


* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Les solutions mises en place

Parmi les propositions suivantes, lesquelles avez-vous mises en place ?

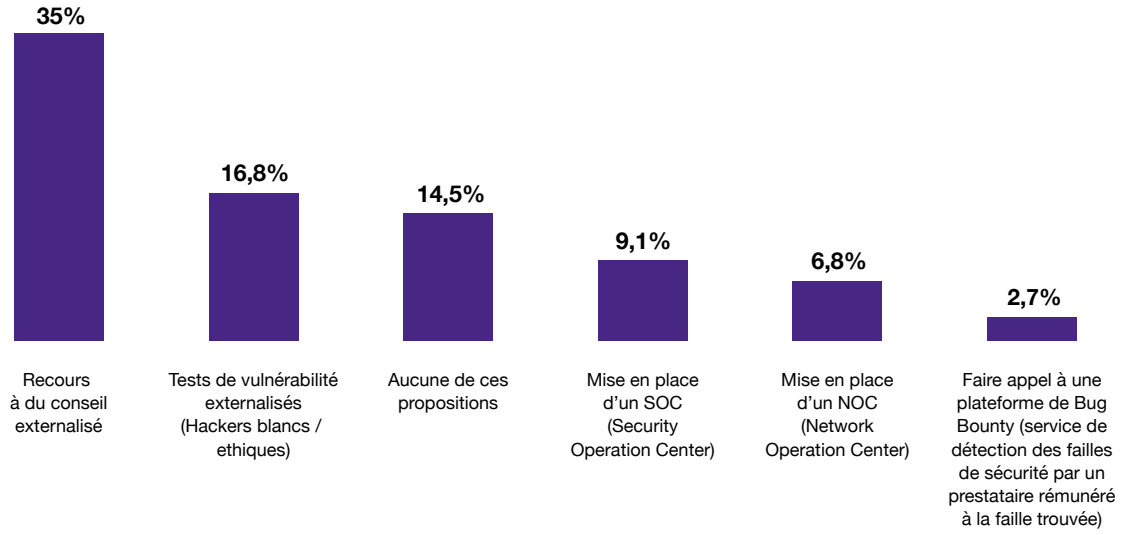


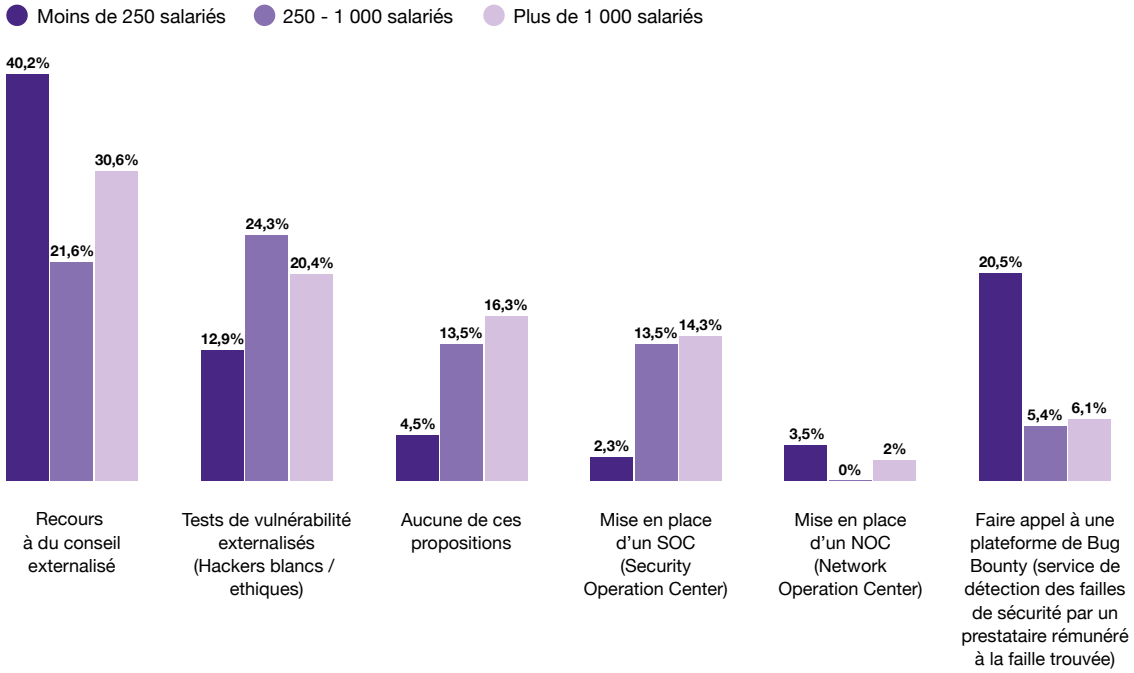


* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Les nouvelles solutions envisagées

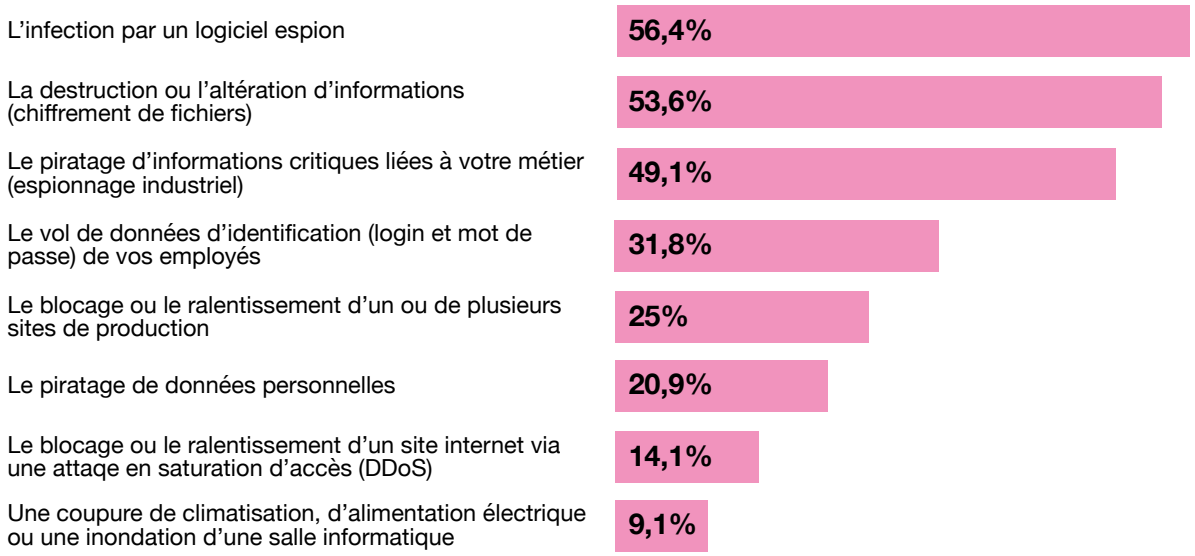
Parmi les propositions suivantes, lesquelles envisagez-vous d'intégrer dans votre stratégie de défense informatique ?

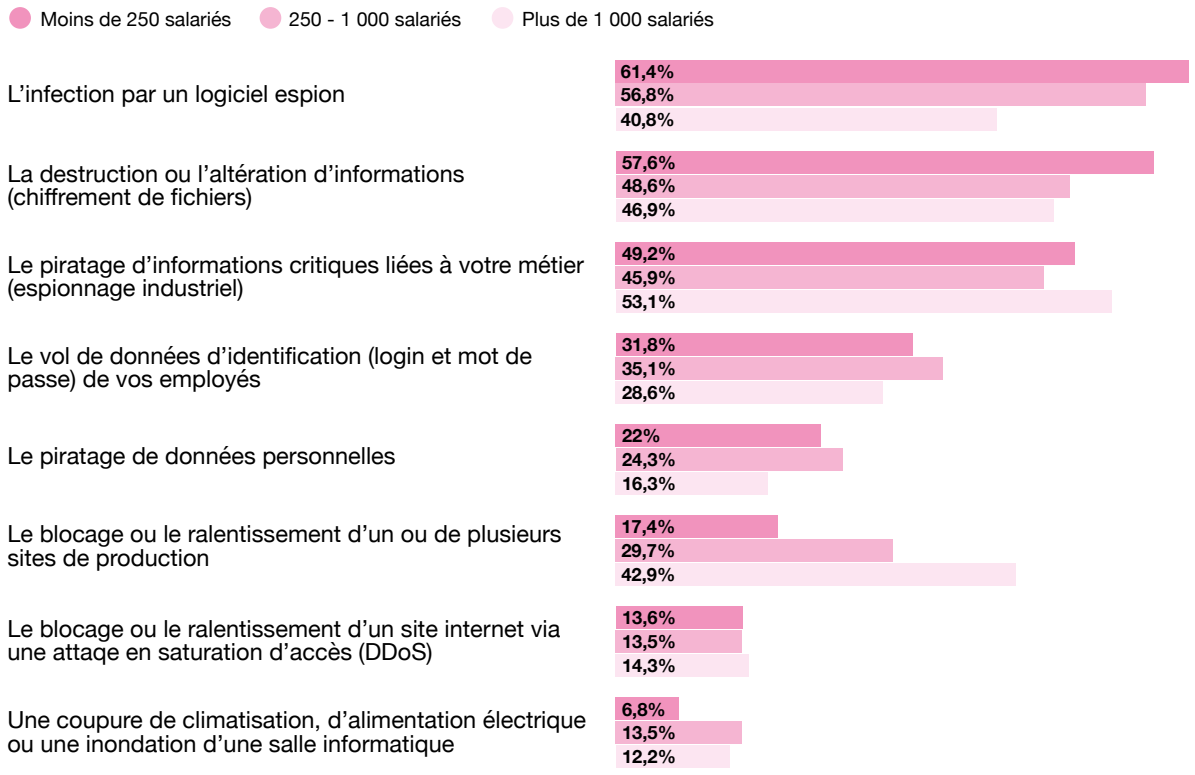




Les types d'attaques les plus redoutées

Parmi les risques suivants, lesquels redoutez-vous le plus ?

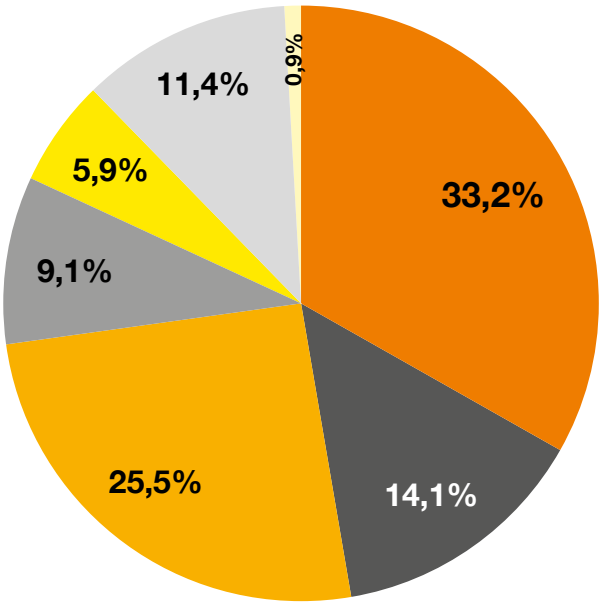


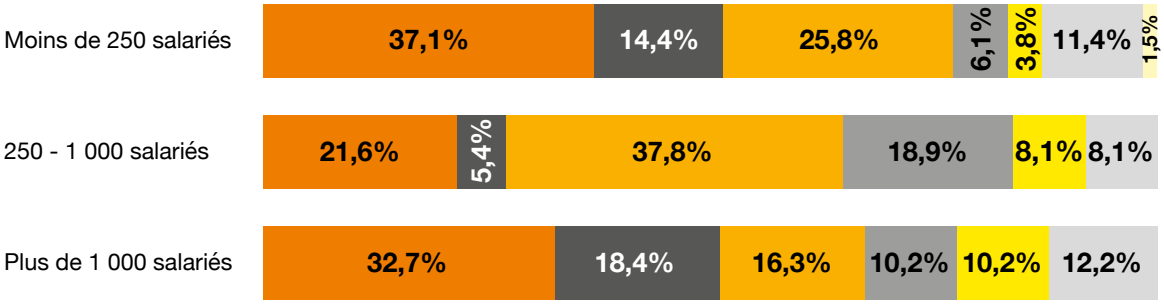


Les principales menaces perçues

Quelle est la menace que vous redoutez le plus en matière de cybersécurité ?

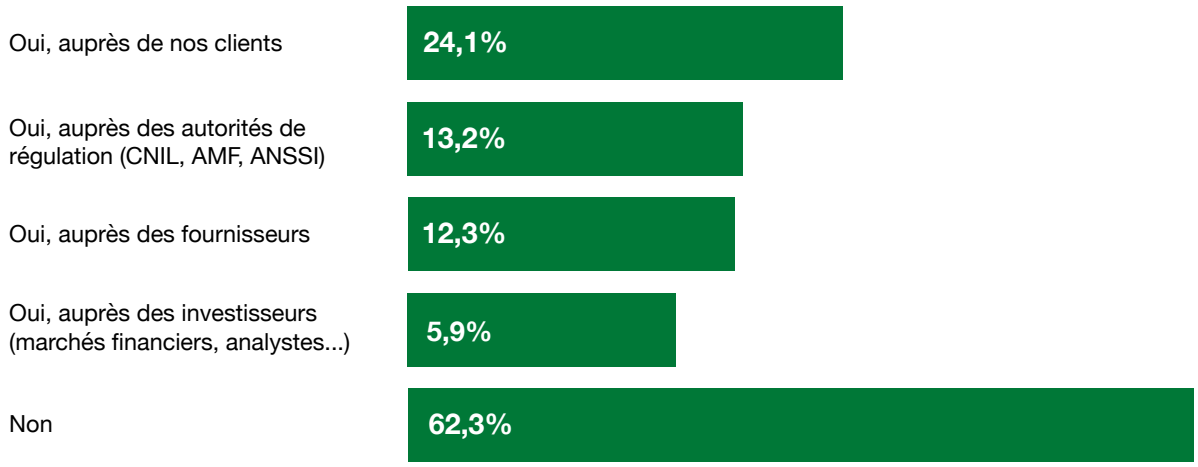
- Virus
- Phishing (hameçonnage)
- Ransomware (logiciel de rançon)
- APT (menaces persistantes avancées, attaques évoluées adaptées à l'écosystème ciblé)
- Ingénierie sociale (récupération de données via les réseaux sociaux...)
- Intrusions physiques au sein de l'entreprise
- Autre





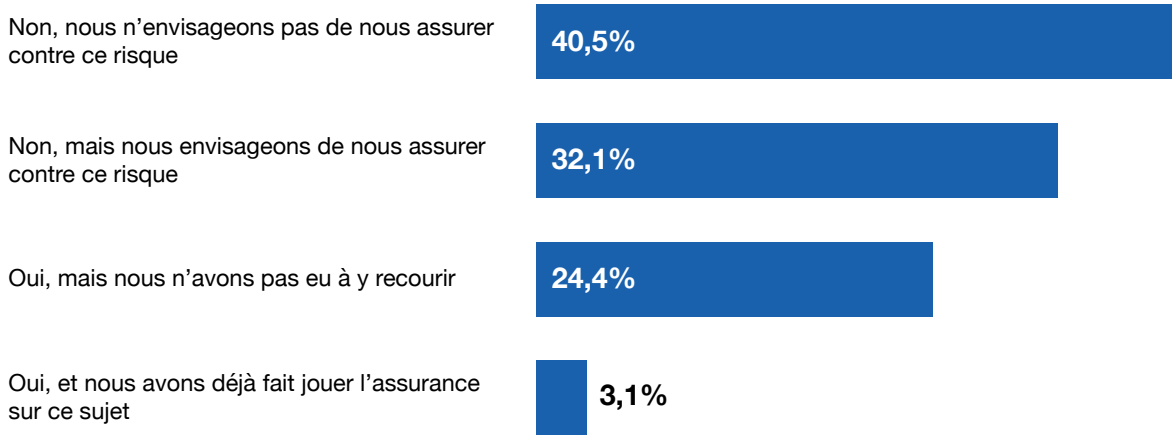
Quelle communication autour de la cybersécurité de l'entreprise ?

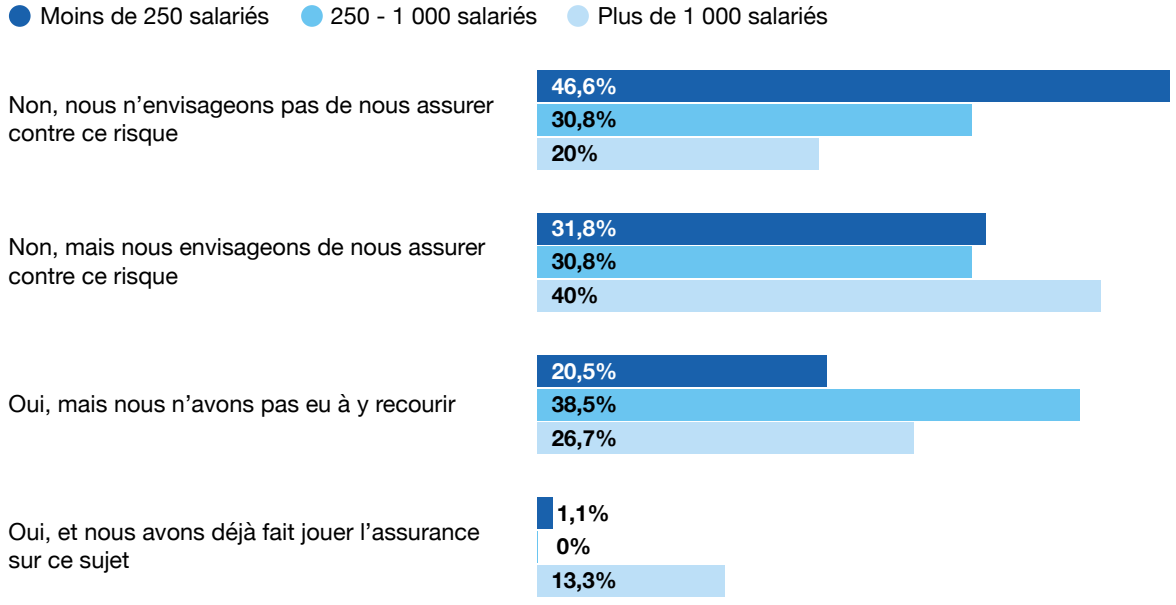
Communiquez-vous sur la politique de cybersécurité de votre entreprise ?



Les entreprises sont-elles assurées ?

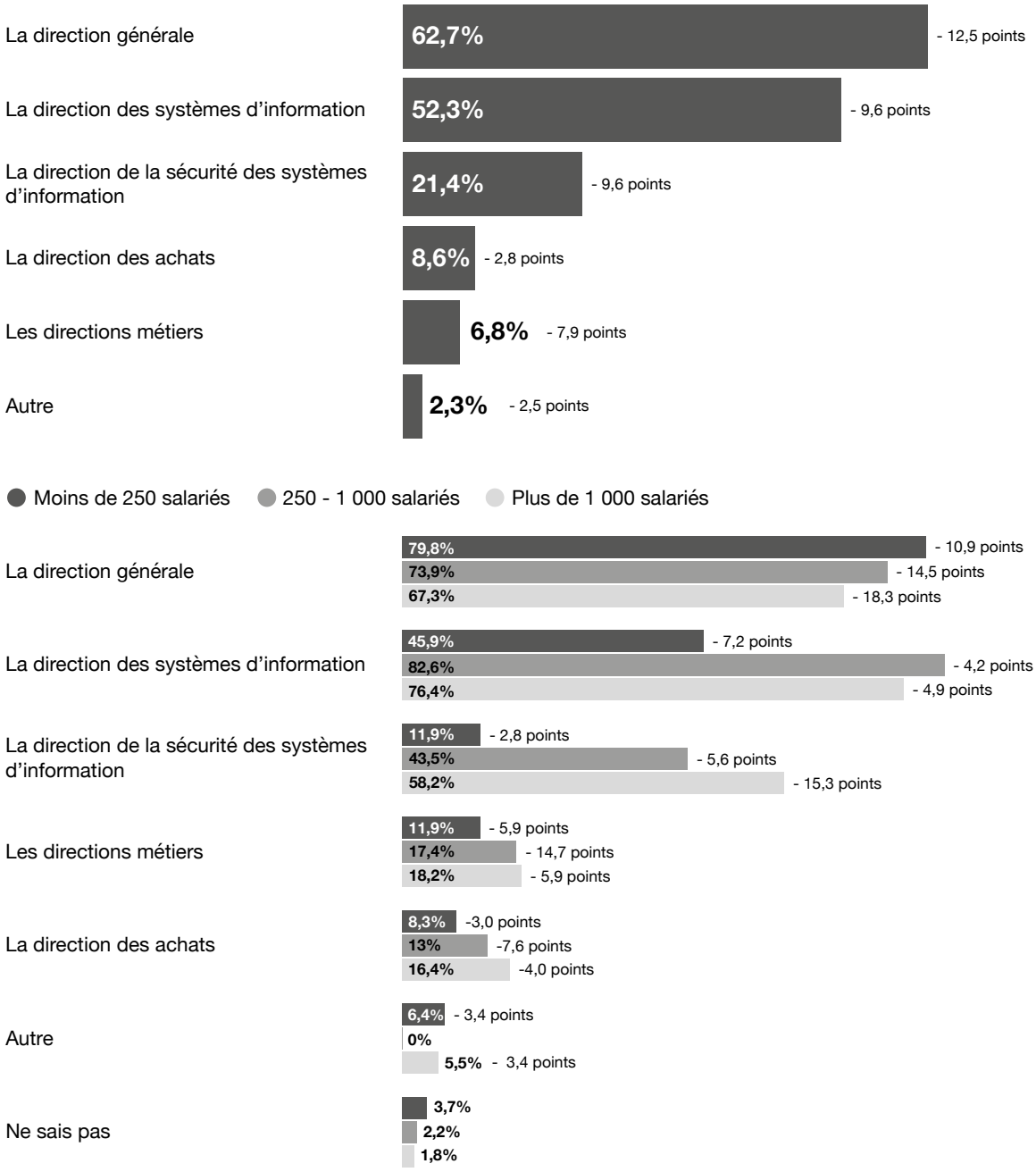
Votre entreprise est-elle assurée contre les risques liés aux défaillances de cybersécurité ?





Les personnes impliquées dans les investissements de sécurité

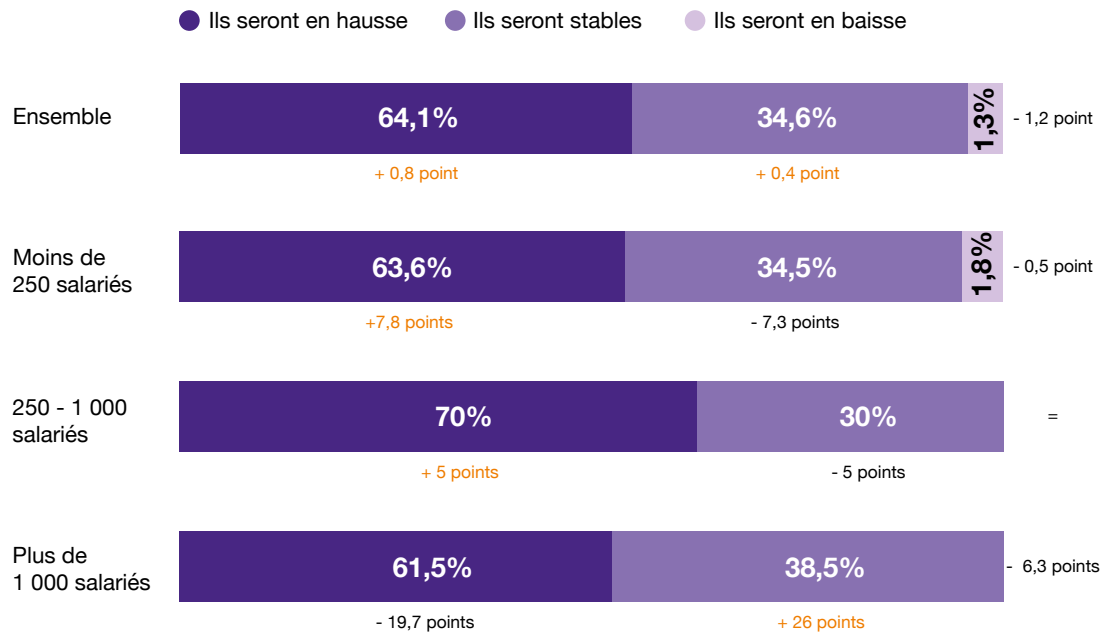
Quelles sont les personnes impliquées dans les investissements de cybersécurité ?



* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Les investissements à venir

Pour finir, comment pensez-vous que les investissements dans la cybersécurité vont évoluer dans les 12 prochains mois ?



* Points d'écart constatés par rapport au Baromètre Cybersécurité 2015.

Décryptage

Quelques points clés à retenir

- Dans cette étude, **plus de la moitié des entreprises interrogées ont déclaré avoir subi une attaque,** mais qu'en est-il dans la réalité ? Aujourd'hui, toutes les entreprises ne sont pas équipées des outils de mesure et de détection des attaques. Il est fort probable que beaucoup d'attaques soient passées complètement inaperçues, ou bien qu'elles ne soient découvertes que bien plus tard.

- Face aux risques de cyberattaques, **on observe une nette différence entre les grandes entreprises et les plus petites**, en matière de préparation et d'investissement. Certes, elles ne bénéficient pas toutes des mêmes moyens financiers et humains, mais surtout, la législation ne s'impose pas à elles de la même manière. Or, le 25 mai 2018, **le General Data Protection Regulation** (GDPR), nouveau règlement européen sur la protection des données personnelles, imposera notamment à tous les organismes privés et publics qui collectent, traitent et stockent des données personnelles, à être transparentes et à alerter les autorités compétentes en cas de constatation d'une fuite de données. Par conséquent, il conviendra de certifier leur système de management de la sécurité informatique, voire d'obtenir la certification ISO 27001.

- On notera également **l'importance de la dimension humaine** : dans l'univers high-tech le volet technologique est important mais le volet humain l'est tout autant. Que ce soit de façon imprudente ou délibérée, avec le développement de la revente de données, du « crime as a service », toutes les entreprises et tous les individus sont concernés.

- L'étude montre clairement **une montée en gamme des attaques** : les hackers recherchent des informations à forte valeur ajoutée, ils ciblent les données les plus sensibles, celles qui sont essentielles à l'entreprise et n'hésitent pas à les « prendre en otage » afin de réclamer des rançons qui peuvent coûter très cher.

- En matière de solution, on observe une forte prise de conscience. Beaucoup de moyens d'actions ont été mis en place, mais ils ne suffisent pas toujours. **Il est nécessaire d'adopter une posture de défense permanente**, avec des outils constamment à jour, de s'entourer d'expertises au fait des toutes dernières tendances et d'avoir une supervision globale de sa cybersécurité.

Conclusion

La spécificité de son IT et sa jeune expérience en matière de sécurité informatique font du secteur industriel, un secteur particulièrement sensible aux cybermenaces, qu'elles soient liées à des erreurs humaines ou des actes de malveillance (augmentation significative des incidents + 4,8 % chez les grandes entreprises et + 9,8 % pour les plus petites). Pour s'assurer la mise en place d'une sécurité optimale, les industriels ont tout intérêt à se faire accompagner par un partenaire reconnu et expert en sécurité industrielle tel qu'Orange Cyberdefense.

Aussi, avec le rachat récent de Lexsi, Orange Cyberdefense a renforcé son expertise dans ce domaine et propose aujourd'hui un accompagnement sur mesure aux entreprises industrielles, que ce soit dans la gestion des IoT, la sensibilisation des collaborateurs ou plus largement la sécurité de leurs systèmes d'information. Une offre s'adressant à la fois aux grandes entreprises et aux plus petites, qui comme on le constate dans cette étude ne se sentent pas suffisamment préparées.

Découvrez les solutions d'Orange Cyberdefense :
www.orange-business.com/fr/securite

orange™ Business Services